PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G07F 7/10, 19/00

A1

(11) International Publication Number: **WO 00/10140**

(43) International Publication Date: 24 February 2000 (24.02.00)

(21) International Application Number: PCT/IL99/00443

(22) International Filing Date: 17 August 1999 (17.08.99)

(30) Priority Data:
125826 17 August 1998 (17.08.98) IL

(71)(72) Applicants and Inventors: SHEM-UR, Jonathan [IL/IL]; Rotshild Blvd. 108, 65271 Tel-Aviv (IL). WOLFSON, Anat [IL/IL]; Uruguay St. 14, 96702 Jerusalem (IL). BAR-LEV, Shaul [IL/IL]; Gilaad St. 11, 52515 Ramat-Gan (IL). SIVAN, Roni [IL/IL]; Paamoni St. 10, 62918 Tel-Aviv (IL). KASHTAN, Ehud [IL/IL]; Somolanski St. 9a, 34368 Haifa (IL).

(74) Agent: NOAM, Meir; P.O. Box 34335, 91342 Jerusalem (IL).

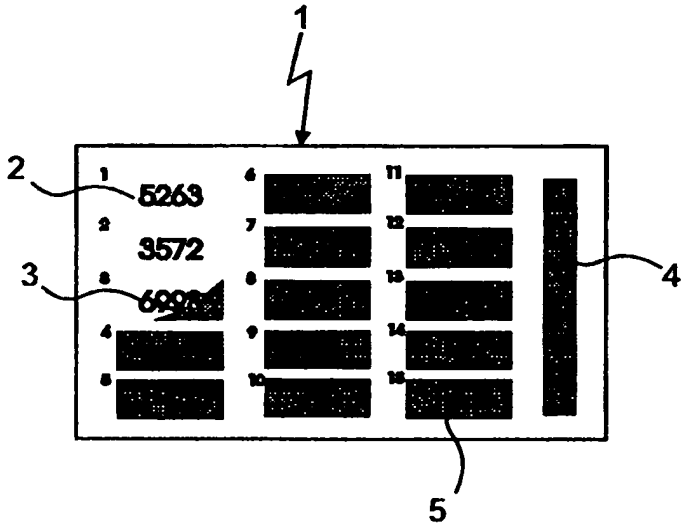
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR PREVENTING UNAUTHORIZED USE OF CREDIT CARDS IN REMOTE PAYMENTS AND AN OPTIONAL SUPPLEMENTAL-CODE CARD FOR USE THEREIN

(57) Abstract

Method for preventing unauthorized use of credit cards in remote payments and a supplemental-code card for use thereof are disclosed. A secret unique code list is provided by the credit company to the credit card owner for use with the credit card. Code lists are distributed to the credit card owners through any acceptable way, such as through automatic teller machines (A.T.M.), code cards sold in stores, E-mail, Fax machines, etc. A copy of each code list is registered in an office of the credit company on the name of its associate credit card owner. Each code is for only a single use. The owner transmits to a creditor one code from his unique list for every separate remote payment, together with the conventional credit card data. The transmitted information is verified through a dialogue between the creditor and the credit company, which accepts or rejects the payment according to the verification result.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD FOR PREVENTING UNAUTHORIZED USE OF CREDIT CARDS IN REMOTE PAYMENTS AND AN OPTIONAL SUPPLEMENTAL-CODE CARD FOR USE THEREIN

Field of the invention

The present invention generally relates to a method for preventing unauthorized use of credit cards in remote payments, and an optional supplemental-code card for use in said method. More specifically, according to the method of the present invention each remote payment is secured by a unique code (for only one time use) which is known only to the credit card owner and to the credit company. According to one preferred embodiment of the present invention, lists of the unique codes are supplied to the credit card owners through automatic-teller machines (hereinafter called also A.T.M). According to another preferred embodiment, the said unique codes are supplied to the credit card owners printed on supplemental-code cards, enable to supply lists of codes confidentially, and help the credit card owners to find out the valid code for each particular remote payment. According to another preferred embodiment the said unique codes are supplied to the credit card owners by any electronic media such as Internet, E-mail etc.

Background of the invention:

Remote payments by credit cards take a constantly growing importance in the world economy. In the conventional credit card remote payments, a credit account is charged according to instructions and credit card details given by the customer, without checking the physical presence of the card in the customer hand. Many people hesitate to use credit card, because its

details can be reached and exploited by unauthorized users. The credit cards companies have no effective way to prevent such illegal use of credit cards by unauthorized users.

The purpose of the present invention is to provide facile and simple method for totally secure remote payments, without changing the conventional credit card held by the user.

The method according to the present invention is for distinguishing between authorized and unauthorized payments, and an optional supplemental-code card can be used in said method together with the conventional credit card. (Another advantage in using the method of the present invention is the avoidance of mistaken payments, such as double charging).

Such protection will encourage the use of credit cards in remote payments, while reducing the losses and the accompanying expenses caused by unauthorized and illegal use.

The method according to the present invention and the optional supplemental-code card can be used also for regular direct credit card payments (i.e. involving presenting the physical credit card by its owner to the creditor), all according to the economic policy of the credit company.

The use of the method according to the present invention will also release the existing psychological inhibitions in working with credit cards, thus increasing their request and usage.

In the context of the present invention:

The term "remote " - relates to a payment performed through communication between a credit card owner and a remote creditor, made by any known physical way such as electrical wires, Radio, optic fiber,

and through any acceptable media such as: phone, Fax machine, mail, interactive television or Internet.

The term "payments" - relates not only to payments, but to any remote activity which is involved with a transmission of valid credit card data, and makes use (or suited to make use) of the protection method of the present invention.

The term: "remote payment" relates to any payment by credit card, using the card data without the presence of the physical card.

The term "code" - relates to any combination of digits or letters.

The term "credit company" relates to any finance or commercial entity supplying remote payments services.

The term "credit card" - relates not only to a concrete physical card but (and especially) to the constant data of a credit account and its owner, which is regularly used to perform conventional remote payments. However, It has to be noted that according to the present invention (and differently from conventional credit card payments), the constant data of a credit card do not have to include a constant identification number, and all the payments can be executed using only the single use codes, together with any constant data predetermined by the credit company as a precondition for accessing the registered code list copy of the specific credit card owner, in the credit company office.

Summary of the invention:

The present invention relates to a method for preventing unauthorized use of credit cards in remote payments comprising the steps of;

(a) providing by a credit company plurality of secret code lists for use with plurality of credit cards, wherein each list is provided to the use of a single owner of at least one credit card, and each code is for only a single use (preferably, the secret codes are generated randomly by an appropriate computer program, as known in the art), and wherein a copy of the code content of each list is registered (preferably stored in a credit computer) in an office of the credit company on the name of its authorized user (hereinafter called "credit card owner").

(b) transmitting one code from said list to a creditor by the credit card owner for every separate remote payment, together with any required conventional data of the credit card, and said single use code is marked by the owner in order to prevent a double use of the same code;

(c) verifying the said single code together with the other conventional credit card data through a dialogue (by either voice, interactive television, by computer, Internet, Fax machine, mail or E-mail) between the creditor and the credit company, and accepting or rejecting the payment, according to the verification result. The said dialogue can be done either between humans, between a human and a machine or automatically between machines without the involvement of humans.

(d) invalidating the single code used for an accepted payment, from the registered code list copy in the credit company office.

According to one preferred embodiment of the invention, the code list is supplied to the credit card owners through the known existing automatic teller machines (A.T.M.). The machine is programmed for producing lists of random codes (or receiving them on-line from the computer of the

credit company), printing them on a voucher for the user, and transmitting them to the credit computer of the credit company for a registration on the name of its authorized user, wherein all said procedure is executed subsequently to the detection of a physical valid automatic-teller card inserted by a user into the machine, and only after typing-on its associate secret code.

According to another preferred embodiment the automatic teller machine (A.T.M.). is programmed for offering the user selecting between some customer options, such as: determining which of the credit card activities will require a supplemental-code; determining the amount of codes in the generated code list; etc.

Actually, the present invention may be thought as providing an advanced credit card type, having a variable card number, varying for every single use of the card. This variable card-number is a combination of the conventional fixed card-number and the single use code.

In another preferred embodiment the present invention provides a supplemental-code card (hereinafter called also "code card") for preventing unauthorized use of credit cards according to the said method, wherein the code card contains a list of codes for use in said method. Preferably, each code is covered by a removable layer of opaque material, for removal by the credit card owner according to a predetermined uncovering progression, prior to performing each remote payment.

The covering material may be a removable sticker (preferably having a free end for facile pulling out), or a scratchable printing paint, or a combination thereof. In the combination, the sticker is covered with a layer of scratchable printing paint such that once it was removed it is permanently damaged, thus a double use or glimpsing the code by frauds is prevented. This combination integrates the advantage of a sticker (i.e.

its facile removal) and the advantage of the scratchable paint (i.e. better confidence).

It has to be noted that the method of the present invention does not rely on any physical code card, and the code list may be supplied to the users through automatic-teller machines (A.T.M.)., through an electronic wallet, through phone by voice, through a mailed letter, or through electrical means such as by facsimile machine, by the Internet, by E-mail or by any other acceptable distribution way.

According to the present invention, the code may be of one character/digit or more (or a combination thereof), according to the required protection level and to other considerations of design.

In terms of credit card security, such 4 digit code may be considered as unbreakable, however there is no prevention to expand it to more than 4 digits, or to use letters additionally to the digit decade.

The number of codes included in one card is a matter of design. According to the present invention a card may include from one code up to several tens of codes (or more), according to the card dimensions, and the size of code characters (font size). The codes may be configured in any wanted form of columns or rows (and may be arranged either from one side or all sides of the card). Preferably, the code list can be designed to be used successively, and the computer of the credit company is programmed such that a non-permitted deviation from the successive order of the codes (there might be also a permitted deviation, all according to the predetermined rules of the credit-card company), disqualifies the whole respective code list. However, according to other embodiments, a non successive use of codes is permitted, provided that they are all of a single list, or more (as will be determined by the credit company).

The supplemental code card can be made of any material, and the codes may be printed or embedded on it in any known method, and in any predetermined configuration.

According to another embodiment, the codes in the card are not covered, however the card is perforated or has a cut near each code, allowing a facile removal or facile marking of used codes, by tearing the relevant perforated portions of the card, in order to prevent double use of codes.

According to one preferred embodiment of the method of the present invention, the codes are coupled in the office of the credit company to specific credit card owners, in advance.

According to other embodiments of the method of the present invention, each code list has its own identification label, and the code lists are distributed to the credit card owners randomly, by mail, stores or other acceptable distribution ways, and their copies in the office are coupled to the record of a specific credit card owner according to a later communication of each owner reporting to the company the label data of a code list to be used.

In order to reduce the memory space needed for storing large scale of code lists (especially when generated in advance for large scale distribution, as hereinbefore said) it is possible to generate the codes by means of a secret computer algorithm such that said identification label of each supplemental-code card is a key for the secret algorithm for generating the list, and such that code lists do not have to be stored in the computer memory (only the key label has to be coupled to the specific owner, wherein each code is computed momentarily for checking the legality of a current remote payment).

Detailed description of the invention:

The present invention will be further described by figures 1 - 4. These figures are solely intend to illustrate some preferred embodiments of the supplemental code card and in no manner intend to limit the scope of the present invention.

Brief description of the figures:

Figure 1 illustrates a card having codes, each of four digits, covered with a scrathable material.

Figure 2 illustrates a card having codes covered with stickers.

Figure 3 illustrates a card having codes covered with stickers and a scratchable material, in combination.

Figure 4 illustrates a card having codes, each of seven digits, covered with stickers.

Figure 1 illustrates a supplemental code card (1) according to the present invention, having 15 codes arranged in three columns. Each code is of four digits (only for example purpose) and covered with a thin layer of a scratchable printing paint (5). Prior to the execution of each payment, the credit card owner has to scratch and remove the cover of another code, and to report it together with the conventional credit card data.

In this figure, the code (2) and the next one, are already used. The valid code for the current payment (3), is illustrated half-scratched. The card has identification number which is also covered (4) with the scratchable material. This number is for reporting to the credit company what card uses the credit card owner. It is helpful in case that the credit company

supplies the owner with more than one code card at a time, or in case that the code card is acquired by the user in a store. If no identification is needed (i.e. one code card is supplied to a credit card owner at a time) the identification number is unnecessary, and the code card do not have to include it.

Figure 2 illustrates a code card (6) having 15 codes, each is covered by a sticker (5). The code (8) and the two next ones, are exposed since they have already been used. The card identification (7) is also exposed. The valid code for the current payment (9) is illustrated during the removal of its sticker, which is seen half separated from the card.

Figure 3 illustrates a code card (11) having 15 codes, each is covered by a combination of both a sticker and a removable layer. The end of the stickers (12) is a tag not covered by the removable layer, thus it can be easily pulled out (15) for removing the sticker. When a sticker is removed, the removable layer is permanently damaged, and the sticker cannot be repaired. Two used codes (14) and the next one, are exposed, and so is the card identification (13).

Figure 4 illustrates a card (16) having codes, each of seven digits, covered with stickers. The secure given by 7 digits (from the statistical perspective) permits using the codes with no obligation to any predetermined order, thus (differently from the cards of figures 1 – 3), no serial numbers are printed adjacent to the stickers. A few used codes, which were used randomly without any successive order, are illustrated (those whose stickers are removed).

The performance of a card having four digit codes as requires a successive order in its use, and of a card having seven digit codes as not requires a successive order in its use, is only for a demonstration

purposes. The actual requirements are subject to the considerations of the credit company.

This card is illustrated without identification number, as an example for a card supplied directly from the credit company to a specific user, thus registered in the company office on the name of the user, in advance.

Claims:

1. Method for preventing unauthorized use of credit cards in remote payments comprising the steps of;

   (a) providing by a credit company plurality of secret code lists for use with plurality of credit cards, wherein each list is provided to the use of a single owner of at least one credit card, and each code is for only a single use, and wherein a copy of the code content of each list is registered in an office of the credit company on the name of its authorized user;

   (b) transmitting one code from said list to a creditor by the credit card owner for every separate remote payment, together with any required conventional data of the credit card, and said single use code is marked by the owner in order to prevent a double use with the same code;

   (c) verifying the said single code together with the other conventional credit card data through a dialogue between the creditor and the credit company, and accepting or rejecting the payment, according to the verification result.

   (d) invalidating the single code used for an accepted payment, from the registered code list copy in the credit company office.

2. Method for preventing unauthorized use of credit cards in remote payments according to claim 1, wherein the code list is supplied to the credit card owners through automatic teller machines, which are programmed for producing lists of random codes, or for receiving lists of random codes on-line from a computer of credit company, printing them on a voucher for the user, and transmitting them to the credit computer of the credit company for a registration on the name

of the authorized user, wherein all said procedure is executed subsequently to the detection of a physical valid credit inserted by a user into the machine, and only after typing-on its associate secret code.

3. Method for preventing unauthorized use of credit cards in remote payments according to claim 2, wherein the automatic teller machines are programmed for offering the user selecting between customer options.

4. Method for preventing unauthorized use of credit cards in remote payments according to claim 1, wherein each code list has its own identification label, and the code lists are distributed to the credit card owners randomly, by mail, stores or other acceptable distribution ways, and their copies in the office are coupled to specific credit card owner, according to a later communication of each owner reporting to the company the label data of a code list to be used.

5. Method for preventing unauthorized use of credit cards in remote payments according to claim 1, wherein the codes are generated randomly by a computer program.

6. Code card for preventing unauthorized use of credit cards in remote payments according to the method defined by claims 1, wherein the card contains a list of codes for use in said method, and each code is covered by a removable layer of opaque material, for removal by the credit card owner according to a predetermined uncovering progression, prior to performing each remote payment.

7. Code card for preventing unauthorized use of credit cards in remote payments according to claim 6 wherein the removable layer is scratchable printing material.

8. Code card for preventing unauthorized use of credit cards in remote payments according to claim 6 wherein the removable layer is a sticker.

9. Code card for preventing unauthorized use of credit cards in remote payments according to claim 6 wherein the removable layer is a combination of a sticker covered by a scratchable printing material and having free tags for facile removal.

10. Code card for preventing unauthorized use of credit cards in remote payments according to the method defined by claims 1, wherein the card contains a list of codes for use in said method, wherein the card is perforated or has a cut near each code, allowing a facile removal or facile marking of used codes by tearing the relevant perforated portions of the card.

11. Code card for preventing unauthorized use of credit cards in remote payments substantially as hereinbefore described and illustrated.

12. Method for preventing unauthorized use of credit cards in remote payments substantially as hereinbefore described.

Figure 1

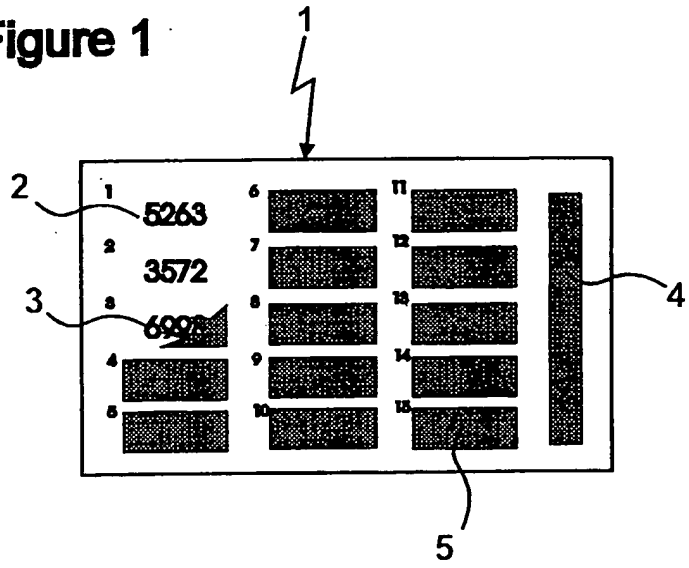


Figure 2

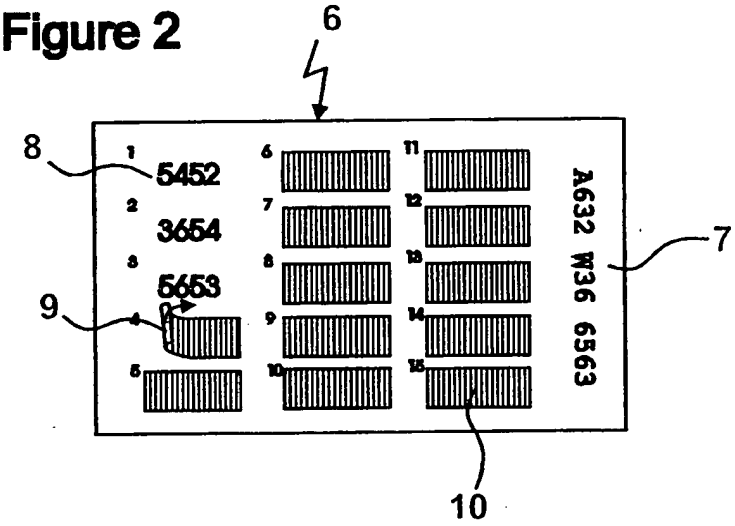


Figure 3

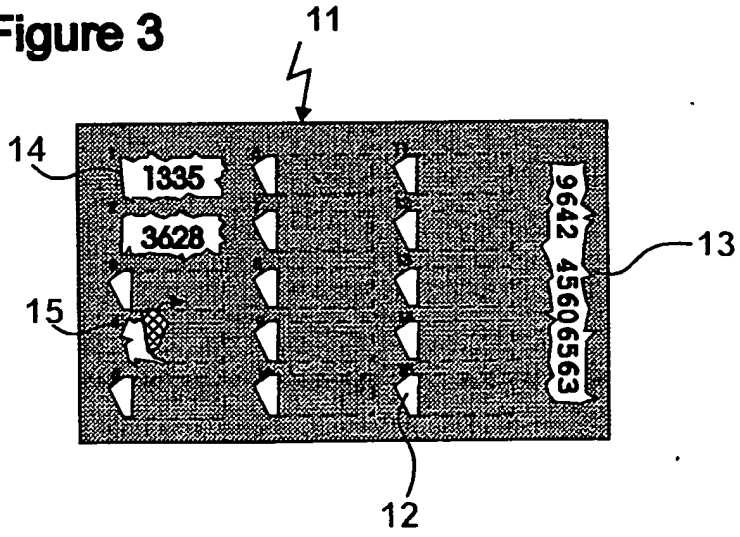
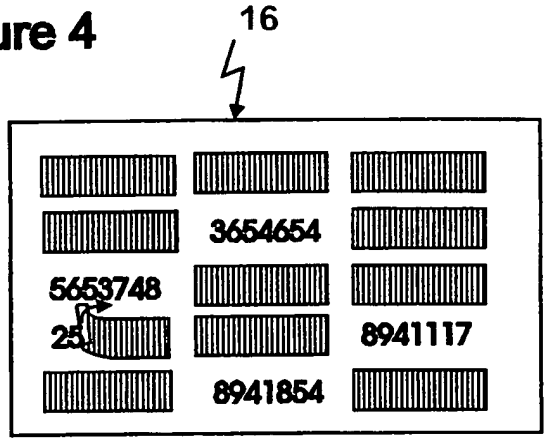


Figure 4



INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/IL 99/00443

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 747 962 A (I. AARON) 31 October 1997 (1997-10-31)	1,6,7
A	the whole document	4
Y	WO 95 34161 A (CALL PROCESSING) 14 December 1995 (1995-12-14) abstract; claims; figures page 13, line 9 -page 14, line 29	1,6,7
Y	GB 2 252 270 A (G.M. WREN-HILTON) 5 August 1992 (1992-08-05)	1,4-6
A	abstract; claims; figures page 12, line 1 -page 18, line 9	7-9,11, 12

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 November 1999	30/11/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/IL 99/00443

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 010 496 A (M. CHATEAU) 30 April 1980 (1980-04-30)	1,4-6
A	abstract; claims; figures page 13, line 32 -page 17, line 24	10
A	WO 97 19549 A (AVERY DENNISON CORPORATION) 29 May 1997 (1997-05-29) the whole document	1-3,5-12
A	WO 95 12169 A (VISA INTERNATIONAL SERVICE ASSOCIATION) 4 May 1995 (1995-05-04)	
A	US 5 696 908 A (K. MUEHLBERGER) 9 December 1997 (1997-12-09)	
A	WO 85 03787 A (P. WHITE) 29 August 1985 (1985-08-29)	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int... ...onal Application No
PCT/IL 99/00443

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2747962 A	31-10-1997	NONE	
WO 9534161 A	14-12-1995	US 5511114 A	23-04-1996
		US 5577109 A	19-11-1996
		AU 2770795 A	04-01-1996
		CA 2192310 A	14-12-1996
		US 5721768 A	24-02-1998
GB 2252270 A	05-08-1992	NONE	
EP 0010496 A	30-04-1980	FR 2439436 A	16-05-1980
WO 9719549 A	29-05-1997	US 5673309 A	30-09-1997
		AU 7738196 A	11-06-1997
WO 9512169 A	04-05-1995	US 5477038 A	19-12-1995
		AU 686276 B	05-02-1998
		AU 1039795 A	22-05-1995
		CA 2174951 A	04-05-1995
		CA 2258830 A	04-05-1995
		EP 0738404 A	23-10-1996
		JP 2897150 B	31-05-1999
		JP 9504396 T	28-04-1997
US 5696908 A	09-12-1997	NONE	
WO 8503787 A	29-08-1985	US 4630201 A	16-12-1986
		CA 1232684 A	09-02-1988
		EP 0172877 A	05-03-1986
		JP 5014298 B	24-02-1993
		JP 61501477 T	17-07-1986